UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/806,510	04/16/2001	Makoto Saito	010321	9318

38834 7590 01/27/2005

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP
1250 CONNECTICUT AVENUE, NW
SUITE 700
WASHINGTON, DC 20036

EXAMINER	
BAUM, RONALD	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 01/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Supplemental **Office Action Summary**	Application No. 09/806,510	Applicant(s) SAITO, MAKOTO	
	Examiner Ronald Baum	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-86* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-86* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This supplemental action corrects minor errors in the action of 12/2/2004 related to:

- incorrect examiner phone number in conclusion
- "Period of reply" error showing "6" instead of "3" months in the PTOL-326 Office Action Summary".

No changes related to the office action examination, references, etc., have been changed.

1. Claims 1-86 are pending for examination.

2. Claims 1-86 are rejected.

Claim Objections

Claims 12,13 are objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim. Claims 12,13 are recited to be dependent on any of claims 9-11, which are further dependent on any of claims 1,2. See MPEP § 608.01(n). Accordingly, the examiner assumes for the sake of applying art that claims 12,13 depend directly on claims 1,2.

Claims 27,28,29 are objected to because of the following informalities: The phrase "digital data *double* using" in claims 27,28,29 and "digital data *double*" in claim 29, is assumed to be "digital data using" in claims 27,28,29 and "digital data" in claim 29. Appropriate correction is required.

Claim 30 is objected to because of the following informalities: The phrase "double re-encrypted digital data;" is assumed to be "double re-encrypted digital data *to be stored*;". Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 30 (and 31-45 by dependency) recites the limitation "decrypting *said* stored second changeable-unchangeable key ...". There is insufficient antecedent basis for this limitation in the claim. The examiner assumes for the sake of applying art that the "to be stored" claim 30 objection correction above will correct the phrase.

Double Patenting

A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101 which states that "whoever invents or discovers any new and useful process ... may obtain a patent therefor ..." (Emphasis added). Thus, the term "same invention," in this context, means an invention drawn to identical subject matter. See *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1894); *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957); and *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

A statutory type (35 U.S.C. 101) double patenting rejection can be overcome by canceling or amending the conflicting claims so they are no longer coextensive in scope. The filing of a terminal disclaimer cannot overcome a double patenting rejection based upon 35 U.S.C. 101.

4. Claims 28,30,47,49 (and 31-45, 50-64 by way of dependency) are rejected under 35 U.S.C. 101 as claiming the same invention as that of claims 27,29,46,48. This is a double patenting rejection and appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-86 are rejected under 35 U.S.C. 102(b) as being anticipated by Davis, U.S. Patent 5,825,879.

6. As per claim 1; "A method for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from encrypted digital data, said method comprising the steps of [Abstract, col. 2,lines 10-col. 8,line 51]: encrypting said decrypted digital data using a changeable key to produce changeable key re-encrypted digital data [i.e., col. 5,lines 5-col. 6,line 41, whereas the SVCP clearly re-encrypts with a user/session/ 'frame data key' (i.e., changeable) prior to frame buffer storage.]; encrypting said changeable key re-encrypted digital data using an unchangeable key in a device to produce changeable-unchangeable keys double re-encrypted digital data to be stored, copied or transferred [col. 6,lines 10-col. 7,line 29, whereas the cryptographic functions in the SVCP IDD portion of the system as broadly interpreted by the examiner clearly encompass both encryption and decryption (i.e., encryption and decryption being the same broad interpretation of encryption per se), and clearly as the SVCP contains digital function, it therefore contains memory storage (i.e., registers, latches, memory, etc; 'storage').]; decrypting said copied, stored or transferred changeable-unchangeable keys double re-encrypted digital data using said unchangeable key to said changeable key re-encrypted digital data; and decrypting said changeable key re-encrypted digital data using said changeable key to said decrypted digital data [col. 2,lines 10-col. 8,line 51, whereas the frame buffer encrypted data

is clearly decrypted by the reverse procedure insofar as the content becomes rendered on a display.].";

Further, as per claim 14; "An apparatus [This claim is the apparatus claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection] for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from encrypted digital data, said apparatus comprising: a changeable key encryption unit for encrypting said decrypted digital data using a changeable key to produce changeable key re-encrypted digital data; an unchangeable key encryption unit for encrypting said changeable key re-encrypted digital data using an unchangeable key in a device to produce changeable-unchangeable keys double re-encrypted digital data to be stored, copied or transferred; an unchangeable key decryption unit for decrypting said copied, stored or transferred changeable-unchangeable keys double re-encrypted digital data using said unchangeable key to said changeable key re-encrypted digital data; and a changeable key decryption unit for decrypting said changeable key re-encrypted digital data using said changeable key to said decrypted digital data.".

7. As per claim 2; "A method for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted, from encrypted digital data, comprising the steps of [This claim is claim 1 whereas the changeable and unchangeable aspects of the keys are reversed. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar

as upon being initialized, it does not change unless a procedure to change is performed. Therefore this claim is rejected for the same reasons provided for the claim 1 rejection]: encrypting said decrypted digital data using an unchangeable key in a device to produce unchangeable key re-encrypted digital data; encrypting said unchangeable key re-encrypted digital data using a changeable key to produce unchangeable-changeable keys double re-encrypted digital data to be stored, copied or transferred; decrypting said copied, stored or transferred unchangeable-changeable keys double re-encrypted digital data using said changeable key to said unchangeable key re-encrypted digital data; and decrypting said unchangeable key re-encrypted digital data using said unchangeable key to said decrypted digital data.";

Further, as per claim 15; "An apparatus [This claim is the apparatus claim for the method claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection] for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from encrypted digital data, said apparatus comprising: a changeable key encryption unit for encrypting said decrypted digital data using a changeable key to produce changeable key re-encrypted digital data; an unchangeable key encryption unit for encrypting said changeable key re-encrypted digital data using an unchangeable key in a device to produce changeable-unchangeable keys double re-encrypted digital data to be stored, copied or transferred; an unchangeable key decryption unit for decrypting said copied, stored or transferred changeable-unchangeable keys double re-encrypted digital data using said unchangeable key to said changeable key re-encrypted digital data; and a changeable key decryption unit for decrypting

said changeable key re-encrypted digital data using said changeable key to said decrypted digital data.".

8. Claim 3 ***additionally recites*** the limitation that; "The method according to claim 1 or 2, wherein said steps of encrypting and decrypting using said changeable key are carried out by a software.". The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2,lines 10-col. 8,line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ' ... encrypting and decrypting using said changeable key are... carried out by a software', versus the SVCP per se being either a hardware or software implementation, or more particularly, "The SVCP may also be built into equipment such as DVDs and CD ROM devices (both clearly software embodiments per se)".);

Further, as per claim 16 ***additionally reciting*** the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection] according to claim 14 or 15, in which encrypting and decrypting using said changeable key are carried out by a software.".

9. Claim 4 ***additionally recites*** the limitation that; "The method according to claim 1 or 2, wherein said steps of encrypting and decrypting using said changeable key are carried out by a hardware.". The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2,lines 10-col. 8,line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ' ... encrypting and

decrypting using said changeable key are... carried out by a hardware', versus the SVCP per se being either a hardware or software implementation.);

Further, as per claim 17 ***additionally reciting*** the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection] according to claim 14 or 15, in which encrypting and decrypting using said changeable key are carried out by a hardware.".

10. Claim 5 ***additionally recites*** the limitation that; "The method according to claim 1 or 2, wherein said changeable key is supplied externally from said device.". The teachings of Davis are directed towards such limitations (i.e., col. 5,lines 5-col. 6,line 41, whereas the SVCP clearly re-encrypts with a user/session/ 'frame data key' (i.e., changeable) prior to frame buffer storage, as broadly interpreted by the examiner would clearly encompass ' ... key is supplied externally from said device ...' insofar as the key is a session key entered externally.);

Further, as per claim 18 ***additionally reciting*** the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection] according to claim 14 or 15, wherein said changeable key is supplied externally from said device.".

11. Claim 6 ***additionally recites*** the limitation that; "The method according to claim 1 or 2, wherein said changeable key is generated in said device.". The teachings of Davis are directed towards such limitations (i.e., col. 5,lines 60-col. 7,line 28, whereas the SVCP " ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly

encompass ' ... key is generated in said device ...' insofar as the key is used in conjunction with internal data transfer.);

Further, as per claim 19 ***additionally reciting*** the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection] according to claim 14 or 15, wherein said changeable key is generated in said device.".

12. Claim 7 ***additionally recites*** the limitation that; "The method according to claim 1 or 2, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a software.". The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2,lines 10-col. 8,line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ' ... encrypting and decrypting using said unchangeable key are... carried out by a software', versus the SVCP per se being either a hardware or software implementation, or more particularly, "The SVCP may also be built into equipment such as DVDs and CD ROM devices (both clearly software embodiments per se)". The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 20 ***additionally reciting*** the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 7 above, and is rejected for the same reasons

provided for the claim 7 rejection] according to claim 14 or 15, in which encrypting and decrypting using said unchangeable key are carried out by a software.".

13. Claim 8 ***additionally recites*** the limitation that; "The method according to claim 1 or 2, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a hardware.". The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2,lines 10-col. 8,line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ' ... encrypting and decrypting using said changeable key are... carried out by a hardware', versus the SVCP per se being either a hardware or software implementation. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 21 ***additionally reciting*** the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 8 above, and is rejected for the same reasons provided for the claim 8 rejection] according to claim 14 or 15, in which encrypting and decrypting using said unchangeable key are carried out by a hardware.".

14. Claim 9 ***additionally recites*** the limitation that; "The method according to claim 1 or 2, wherein said unchangeable key is already placed in said device.". The teachings of Davis are directed towards such limitations (i.e., col. 5,lines 60-col. 7,line 28, whereas the SVCP " ...

using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ' ... key is already placed in said device ...' insofar as the key is used in conjunction with internal data transfer. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 22 ***additionally reciting*** the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 9 above, and is rejected for the same reasons provided for the claim 9 rejection] according to claim 14 or 15, wherein said unchangeable key is already placed in said device.".

15. Claim 10 ***additionally recites*** the limitation that; "The method according to claim 1 or 2, wherein said unchangeable key is generated in said device.". The teachings of Davis are directed towards such limitations (i.e., col. 5,lines 60-col. 7,line 28, whereas the SVCP " ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ' ... key is generated in said device ...' insofar as the key is used in conjunction with internal data transfer. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 23 ***additionally reciting*** the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 10 above, and is rejected for the same reasons provided for the claim 10 rejection] according to claim 14 or 15, wherein said unchangeable key is generated in said device.".

16. Claim 11 ***additionally recites*** the limitation that; "The method according to claim 1 or 2, wherein said unchangeable key is supplied externally from said device.". The teachings of Davis are directed towards such limitations (i.e., col. 5,lines 5-col. 6,line 41, whereas the SVCP clearly re-encrypts with a user/session/ 'frame data key' prior to frame buffer storage, as broadly interpreted by the examiner would clearly encompass ' ... key is supplied externally from said device ...' insofar as the key is a session key entered externally. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 24 ***additionally reciting*** the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 11 above, and is rejected for the same reasons provided for the claim 11 rejection] according to claim 14 or 15, wherein said unchangeable key is supplied externally from said device.".

17. Claim 12 ***additionally recites*** the limitation that; "The method according to claim 9, 10 or 11, wherein said unchangeable key is specific to said device.". The teachings of Davis are

directed towards such limitations (i.e., col. 5,lines 60-col. 7,line 28, whereas the SVCP " ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ' ... key is specific to said device ...' insofar as the key is used in conjunction with internal data transfer. Also, the SVCP is applicable to set-top box configurations which inherently have device Ids (i.e., embedded) as part of the processor PROM/ROM type memory. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 25 ***additionally reciting*** the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 12 above, and is rejected for the same reasons provided for the claim 12 rejection] according to claim 14 or 15, wherein said unchangeable key is specific to said device.".

18. Claim 13 ***additionally recites*** the limitation that; "The method according to claim 9, 10 or 11, wherein said unchangeable key is not specific to said device.". The teachings of Davis are directed towards such limitations (i.e., col. 5,lines 60-col. 7,line 28, whereas the SVCP " ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ' ... key is not specific to said device ...' insofar as the key is used in conjunction with internal data transfer. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable)

insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 26 ***additionally reciting*** the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 13 above, and is rejected for the same reasons provided for the claim 13 rejection] according to claim 14 or 15, wherein said unchangeable key is not specific to said device.".

19. As per claim 27; "A method for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said method comprising the steps of [Abstract, col. 2,lines 10-col. 8,line 51]: encrypting said decrypted digital data using a second changeable key to produce second changeable key re-encrypted digital data [i.e., col. 5,lines 5-col. 6,line 41, whereas the SVCP clearly re-encrypts with a user/session/ 'frame data key' (i.e., changeable) prior to frame buffer storage.]; encrypting said second changeable key re-encrypted digital data using an unchangeable key in a device to produce unchangeable-second changeable keys double re-encrypted digital data to be stored [col. 6,lines 10-col. 7,line 29, whereas the cryptographic functions in the SVCP IDD portion of the system as broadly interpreted by the examiner clearly encompass both encryption and decryption (i.e., encryption and decryption being the same broad interpretation of encryption per se), and clearly as the SVCP contains digital function, it therefore contains memory storage (i.e., registers, latches, memory, etc; 'storage').]; decrypting said stored unchangeable-second changeable keys double re-encrypted digital data using said unchangeable key to said second

changeable key re-encrypted digital data; encrypting said second changeable key re-encrypted digital data using a third changeable key to produce third changeable-second changeable keys double re-encrypted digital data to be copied or transferred [col. 2,lines 10-col. 8,line 51, whereas this is the aspect that deals with the intermediate storage/transfer to intervening memory/storage elements. The SVCP network embodiments clearly encompass this aspect, as broadly interpreted by the examiner.]; decrypting said copied or transferred third changeable-second changeable keys double re-encrypted digital data double using said third changeable key to said second changeable key re-encrypted digital data; and decrypting said second changeable key re-encrypted digital data using said second changeable key to said decrypted digital data [col. 2,lines 10-col. 8,line 51, whereas the frame buffer encrypted data is clearly decrypted by the reverse procedure insofar as the content becomes rendered on a display.].";

Further, as per claim 46; "An apparatus [This claim is the method claim for the apparatus claim 27 above, and is rejected for the same reasons provided for the claim 27 rejection] for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said apparatus comprising: a second changeable key encryption unit for encrypting said decrypted digital data using a second changeable key to produce second changeable key re-encrypted digital data; an unchangeable key encryption unit for encrypting said second changeable key re-encrypted digital data using an unchangeable key in a device to produce unchangeable-second changeable keys double re-ncrypted digital data to be stored; an unchangeable key decryption unit for decrypting said stored unchangeable-second changeable keys double re-encrypted digital data using said unchangeable key to said second changeable key re-encrypted digital data; a third changeable key encryption

unit for encrypting said second changeable key re-encrypted digital data using a third changeable key to produce third changeable-second changeable keys double re-encrypted digital data to be copied or transferred; a third changeable key decryption unit for decrypting said copied or transferred third changeable-second changeable keys double re-encrypted digital data using said third changeable key to said second changeable key re-encrypted digital data; and a second changeable key decryption unit for decrypting said second changeable key re-encrypted digital data using said second changeable key to said decrypted digital data.".

20. As per claim 28; "A method for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said method comprising the steps of [see ***double patenting*** section above above]: encrypting said decrypted digital data using a second changeable key to produce second changeable key re-encrypted digital data; encrypting said second changeable key re-encrypted digital data using an unchangeable key in a device to produce unchangeable-second changeable keys double re-encrypted digital data to be stored; decrypting said stored unchangeable-second changeable keys double re-encrypted digital data double using said unchangeable key to said second changeable key re-encrypted digital data; encrypting said second changeable key re-encrypted digital data using a third changeable key to produce third changeable-second changeable keys double re-encrypted digital data to be copied or transferred; decrypting said copied or transferred third changeable-second changeable keys double re-encrypted digital data double using said third changeable key to said second changeable key re-encrypted digital data; and decrypting said

second changeable key re-encrypted digital data using said second changeable key to said decrypted digital data.";

Further, as per claim 47; "An apparatus [see ***double patenting*** section above above, this claim is the method claim for the apparatus claim 28 above, and is rejected for the same reasons provided for the claim 28 rejection] for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said apparatus comprising: a second changeable key encryption unit for encrypting said decrypted digital data using a second changeable key to produce second changeable key re-encrypted digital data; an unchangeable key encryption unit for encrypting said second changeable key re-encrypted digital data using an unchangeable key in a device to produce unchangeable-second changeable keys double re-encrypted digital data to be stored; an unchangeable key decryption unit for decrypting said stored unchangeable-second changeable keys double re-encrypted digital data using said unchangeable key to said second changeable key re-encrypted digital data; a third changeable key encryption unit for encrypting said second changeable key re-encrypted digital data using a third change-able key to produce third changeable-second changeable keys double re-encrypted digital data [double re-encrypted by third-changeable-second-changeable keys] to be copied or transferred; a third changeable key decryption unit for decrypting said copied or transferred third changeable-second changeable keys double re-encrypted digital data using said third changeable key to said second changeable key re-encrypted digital data; and a second changeable key decryption unit for decrypting said second changeable key re-encrypted digital data using said second changeable key to said decrypted digital data.".

21. As per claim 29; "A method for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said method comprising the steps of [This claim is claim 27 whereas the changeable and unchangeable aspects of the keys are reversed. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed. Therefore this claim is rejected for the same reasons provided for the claim 27 rejection]: encrypting said decrypted digital data using an unchangeable key in a device to produce unchangeable key re-encrypted digital data, and encrypting said unchangeable key re-encrypted digital data using a second changeable key to produce second changeable-unchangeable keys double re-encrypted digital data double to be stored; decrypting said stored second changeable-unchangeable keys double re-encrypted digital data double using said second changeable key to said unchangeable key re-encrypted digital data; decrypting said unchangeable key re-encrypted digital data using said unchangeable key to said decrypted digital data; encrypting said decrypted digital data using a third changeable key to produce third changeable key re-encrypted digital data, and encrypting said third changeable key re-encrypted digital data using said second changeable key to produce second changeable-third changeable keys double re-encrypted digital data to be copied or transferred; decrypting said copied or transferred second changeable-third changeable keys double re-encrypted digital data using said second changeable

key to said third changeable key re-encrypted digital data; and decrypting said third changeable key re-encrypted digital data using said third changeable key to said decrypted digital data.";

Further, as per claim 48; "An apparatus [This claim is the method claim for the apparatus claim 29 above, and is rejected for the same reasons provided for the claim 29 rejection] for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said apparatus comprising: an unchangeable key encryption unit for encrypting said decrypted digital data using an unchangeable key in a device to produce unchangeable key re-encrypted digital data, and a second changeable key encryption unit for encrypting said unchangeable key re-encrypted digital data using a second changeable key to produce second changeable-unchangeable keys double re-encrypted digital data to be stored; a second changeable key decryption unit for decrypting said stored second changeable-unchangeable keys double re-encrypted digital data using said second changeable key to said unchangeable key re-encrypted digital data, and an unchangeable key decryption unit for decrypting said unchangeable key re-encrypted digital data using said unchangeable key to said decrypted digital data; a third changeable key encryption unit for encrypting said decrypted digital data using a third changeable key to produce third changeable key re-encrypted digital data, and a second changeable key encryption unit for encrypting said third changeable key re-encrypted digital data using said second changeable key to produce second changeable-third changeable keys double re-encrypted digital data to be copied or transferred; and a second changeable key decryption unit for decrypting said copied or transferred second changeable-third changeable keys double re-encrypted digital data using said second changeable key to said third changeable key re-encrypted digital data, and a third

changeable key decryption unit for decrypting said third changeable keys re-encrypted digital data using said third changeable key to said decrypted digital data.".

22. As per claim 30; "A method for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said method comprising the steps of [see ***double patenting*** section above above]: encrypting said decrypted digital data using an unchangeable key in a device to produce unchangeable key re-encrypted digital data, and encrypting said unchangeable key re-encrypted digital data using a second changeable key to produce second changeable-unchangeable keys double re-encrypted digital data; decrypting said stored second changeable-unchangeable keys double re-encrypted digital data using said second changeable key to said unchangeable key re-encrypted digital data; decrypting said unchangeable key re-encrypted digital data using said unchangeable key to said decrypted digital data; encrypting said decrypted digital data using a third changeable key to produce third changeable key re-encrypted digital data, and encrypting said third changeable key re-encrypted digital data using said second changeable key to produce second changeable-third changeable keys double re-encrypted digital data to be copied or transferred; decrypting said copied or transferred second changeable-third changeable keys double re-encrypted digital data using said second changeable key to said third changeable key re-encrypted digital data; and decrypting said third changeable key re-encrypted digital data using said third changeable key to said decrypted digital data.";

Further, as per claim 49; "An apparatus [see ***double patenting*** section above above, this claim is the method claim for the apparatus claim 30 above, and is rejected for the same reasons

provided for the claim 30 rejection] for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said apparatus comprising: an unchangeable key encryption unit for encrypting said decrypted digital data using an unchangeable key in a device to produce unchangeable key re-encrypted digital data, and a second changeable key encryption unit for encrypting said unchangeable key re-encrypted digital data using a second changeable key to produce second changeable-unchangeable keys double re-encrypted digital data to be stored; a second changeable key decryption unit for decrypting said stored second changeable-unchangeable keys double re-encrypted digital data using said second changeable key to said unchangeable key re-encrypted digital data, and an unchangeable key decryption unit for decrypting said unchangeable key re-encrypted digital data using said unchangeable key to said decrypted digital data; a third changeable key encryption unit for encrypting said decrypted digital data using a third changeable key to produce third changeable key re-encrypted digital data, and a second changeable key encryption unit for encrypting said third changeable key re-encrypted digital data using said second changeable key to produce second changeable-third changeable keys double re-encrypted digital data to be copied or transferred; and a second changeable key decryption unit for decrypting said copied or transferred second changeable-third changeable keys double; re-encrypted digital data using said second changeable key to said third changeable key re-encrypted digital data, and a third changeable key decryption unit for decrypting said third changeable key re-encrypted digital data using said third changeable key to said decrypted digital data.".

23. Claim 31 ***additionally recites*** the limitation that; "The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting using said second changeable key are carried out by a software.". The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2,lines 10-col. 8,line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ' ... encrypting and decrypting using said changeable key are... carried out by a software', versus the SVCP per se being either a hardware or software implementation, or more particularly, "The SVCP may also be built into equipment such as DVDs and CD ROM devices (both clearly software embodiments per se)".);

Further, as per claim 50 ***additionally reciting*** the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 31 above, and is rejected for the same reasons provided for the claim 31 rejection] according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting using said second changeable key are carried out by a software.".

24. Claim 32 ***additionally recites*** the limitation that; "The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting using said second changeable key are carried out by a hardware.". The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2,lines 10-col. 8,line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ' ... encrypting and decrypting using said changeable key are... carried out by a hardware', versus the SVCP per se being either a hardware or software implementation.);

Further, as per claim 51 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 32 above, and is rejected for the same reasons provided for the claim 32 rejection] according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting using said second changeable key are carried out by a hardware.".

25. Claim 33 ***additionally recites*** the limitation that; "The method according to claim 27, 28, 29 or 30, wherein said second changeable key is supplied externally from said device.". The teachings of Davis are directed towards such limitations (i.e., col. 5,lines 5-col. 6,line 41, whereas the SVCP clearly re-encrypts with a user/session/ 'frame data key' (i.e., changeable) prior to frame buffer storage, as broadly interpreted by the examiner would clearly encompass ' ... key is supplied externally from said device ...' insofar as the key is a session key entered externally.);

Further, as per claim 52 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 33 above, and is rejected for the same reasons provided for the claim 33 rejection] according to claim 46, 47, 48 or 49, wherein said second changeable key is supplied externally from said device.".

26. Claim 34 ***additionally recites*** the limitation that; "The method according to claim 27, 28, 29 or 30, wherein said second changeable key is generated in said device.". The teachings of Davis are directed towards such limitations (i.e., col. 5,lines 60-col. 7,line 28, whereas the SVCP " ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner

would clearly encompass ' ... key is generated in said device ...' insofar as the key is used in conjunction with internal data transfer.);

Further, as per claim 53 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 34 above, and is rejected for the same reasons provided for the claim 34 rejection] according to claim 46, 47, 48 or 49, wherein said second changeable key is generated in said device.".

27. Claim 35 ***additionally recites*** the limitation that; "The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting using said third changeable key are carried out by a software.". The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2,lines 10-col. 8,line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ' ... encrypting and decrypting using said changeable key are... carried out by a software', versus the SVCP per se being either a hardware or software implementation, or more particularly, "The SVCP may also be built into equipment such as DVDs and CD ROM devices (both clearly software embodiments per se)".);

Further, as per claim 54 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 35 above, and is rejected for the same reasons provided for the claim 35 rejection] according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting using said third changeable key are carried out by a software.".

28. Claim 36 ***additionally recites*** the limitation that; "The method according to claim 27, 28, 29 or 30, wherein said steps of re-encrypting and decrypting using said third changeable key are carried out by a hardware.". The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2,lines 10-col. 8,line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ' ... encrypting and decrypting using said changeable key are... carried out by a hardware', versus the SVCP per se being either a hardware or software implementation.);

Further, as per claim 55 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 36 above, and is rejected for the same reasons provided for the claim 36 rejection] according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting using said third changeable key are carried out by a hardware.".

29. Claim 37 ***additionally recites*** the limitation that; "The method according to claim 27, 28, 29 or 30, wherein said third changeable key is supplied externally from said device.". The teachings of Davis are directed towards such limitations (i.e., col. 5,lines 5-col. 6,line 41, whereas the SVCP clearly re-encrypts with a user/session/ 'frame data key' (i.e., changeable) prior to frame buffer storage, as broadly interpreted by the examiner would clearly encompass ' ... key is supplied externally from said device ...' insofar as the key is a session key entered externally.);

Further, as per claim 56 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 37 above, and is rejected for the same reasons

provided for the claim 37 rejection] according to claim 46, 47, 48 or 49, wherein said third changeable key is supplied externally from said device.".

30. Claim 38 ***additionally recites*** the limitation that; "The method according to claim 27, 28, 29 or 30, wherein said third changeable key is generated in said device.". The teachings of Davis are directed towards such limitations (i.e., col. 5,lines 60-col. 7,line 28, whereas the SVCP " ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ' ... key is generated in said device ...' insofar as the key is used in conjunction with internal data transfer.);

Further, as per claim 57 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 38 above, and is rejected for the same reasons provided for the claim 38 rejection] according to claim 46, 47, 48 or 49, wherein said third changeable key is generated in said device.".

31. Claim 39 ***additionally recites*** the limitation that; "The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a software.". The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2,lines 10-col. 8,line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ' ... encrypting and decrypting using said unchangeable key are... carried out by a software', versus the SVCP per se being either a hardware or software implementation, or more particularly, "The SVCP may also be built into equipment such as DVDs and CD ROM devices (both clearly

software embodiments per se)". The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 58 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 39 above, and is rejected for the same reasons provided for the claim 39 rejection] according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a software.".

32. Claim 40 ***additionally recites*** the limitation that; "The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a hardware.". The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2,lines 10-col. 8,line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ' ... encrypting and decrypting using said changeable key are... carried out by a hardware', versus the SVCP per se being either a hardware or software implementation. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 59 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 40 above, and is rejected for the same reasons provided for the claim 40 rejection] according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a hardware.".

33. Claim 41 ***additionally recites*** the limitation that; "The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is already placed in said device.". The teachings of Davis are directed towards such limitations (i.e., col. 5,lines 60-col. 7,line 28, whereas the SVCP " ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ' ... key is already placed in said device ...' insofar as the key is used in conjunction with internal data transfer. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 60 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 41 above, and is rejected for the same reasons provided for the claim 41 rejection] according to claim 46, 47, 48 or 49, wherein said unchangeable key is already placed in the device.".

34. Claim 42 ***additionally recites*** the limitation that; "The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is generated in said device.". The teachings of

Davis are directed towards such limitations (i.e., col. 5,lines 60-col. 7,line 28, whereas the SVCP " ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ' ... key is generated in said device ...' insofar as the key is used in conjunction with internal data transfer. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 61 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 42 above, and is rejected for the same reasons provided for the claim 42 rejection] according to claim 46, 47, 48 or 49, wherein said unchangeable key is generated in the device.".

35. Claim 43 ***additionally recites*** the limitation that; "The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is supplied externally from said device.". The teachings of Davis are directed towards such limitations (i.e., col. 5,lines 5-col. 6,line 41, whereas the SVCP clearly re-encrypts with a user/session/ 'frame data key' prior to frame buffer storage, as broadly interpreted by the examiner would clearly encompass ' ... key is supplied externally from said device ...' insofar as the key is a session key entered externally. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable

from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 62 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 43 above, and is rejected for the same reasons provided for the claim 43 rejection] according to claim 46, 47, 48 or 49, wherein said unchangeable key is supplied externally from the device.".

36. Claim 44 ***additionally recites*** the limitation that; "The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is specific to said device.". The teachings of Davis are directed towards such limitations (i.e., col. 5,lines 60-col. 7,line 28, whereas the SVCP " ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ' ... key is specific to said device ...' insofar as the key is used in conjunction with internal data transfer. Also, the SVCP is applicable to set-top box configurations which inherently have device Ids (i.e., embedded) as part of the processor PROM/ROM type memory. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 63 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 44 above, and is rejected for the same reasons

provided for the claim 44 rejection] according to claim 46, 47, 48 or 49, wherein said unchangeable key is specific to said device.".

37. Claim 45 ***additionally recites*** the limitation that; "The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is not specific to said device". The teachings of Davis are directed towards such limitations (i.e., col. 5,lines 60-col. 7,line 28, whereas the SVCP " ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ' ... key is not specific to said device ...' insofar as the key is used in conjunction with internal data transfer. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 64 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 45 above, and is rejected for the same reasons provided for the claim 45 rejection] according to claim 46, 47, 48 or 49, wherein said unchangeable key is not specific to said device.".

38. As per claim 65; "A method for protecting digital data from illegitimate use, said method comprising the steps of [This claim is claim 1 whereas the changeable and unchangeable aspects of the keys are reversed, and the application specific aspect of licensing (i.e., the 'determining whether said digital data is subject to be protected or not' below). The examiner broadly

interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed. Also, the SVCP clearly determines protection criteria insofar as the SVCP ' ... may be necessary to gain prior authorization before viewing of particular video... ' (i.e., col. 3,lines 13-26). Therefore this claim is rejected for the same reasons provided for the claim 1 rejection]: determining whether said digital data is subject to be protected or not; encrypting said digital data determined to be protected, using an unchangeable key in a device to produce unchangeable key encrypted digital data; storing, copying or transferring said unchangeable key encrypted digital data; decrypting said stored, copied or transferred unchangeable key encrypted digital data using said unchangeable key to said decrypted digital data; and utilizing said stored, copied or transferred unchangeable key encrypted digital data and said decrypted digital data.";

Further, as per claim 76; "An apparatus [This claim is the method claim for the apparatus claim 65 above, and is rejected for the same reasons provided for the claim 65 rejection] for protecting digital data from illegitimate use, said apparatus comprising: determining means for determining whether said digital data is subject to be protected or not; means for encrypting said digital data, determined being subject to be protected, using an unchangeable key in a device to produce unchangeable key encrypted digital data; means for storing, copying or transferring said unchangeable key encrypted digital data; means for decrypting said stored, copied or transferred unchangeable key encrypted digital data to said decrypted digital data; and means for utilizing

said stored, copied or transferred unchangeable key encrypted digital data and said decrypted digital data.".

39. Claim 66 ***additionally recites*** the limitation that; "The method according to claim 65, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a software.". The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2,lines 10-col. 8,line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ' ... encrypting and decrypting using said unchangeable key are... carried out by a software', versus the SVCP per se being either a hardware or software implementation, or more particularly, "The SVCP may also be built into equipment such as DVDs and CD ROM devices (both clearly software embodiments per se)". The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 77 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 66 above, and is rejected for the same reasons provided for the claim 66 rejection] according to claim 76, wherein encrypting and decrypting using said unchangeable key a-re carried out by a software.".

40. Claim 67 ***additionally recites*** the limitation that; "The method according to claim 65, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a hardware.". The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2,lines 10-col. 8,line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ' ... encrypting and decrypting using said changeable key are... carried out by a hardware', versus the SVCP per se being either a hardware or software implementation. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 78 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 67 above, and is rejected for the same reasons provided for the claim 67 rejection] according to claim 76, wherein encrypting and decrypting using said unchangeable key are carried out by a hardware.".

41. Claim 68 ***additionally recites*** the limitation that; "The method according to claim 65, in which encrypting and decrypting using said unchangeable key are controlled by identifying information which is added to said digital data.". The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2,lines 10-col. 8,line 51, whereas, the SVCP clearly determines identifying criteria insofar as the SVCP ' ... may be necessary to gain prior authorization before viewing of particular video... ' (i.e., col. 3,lines 13-26), as broadly

interpreted by the examiner would clearly encompass ' ... controlled by identifying information ...'.);

Further, as per claim 79 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 68 above, and is rejected for the same reasons provided for the claim 68 rejection] according to claim 76, wherein encrypting and decrypting using said unchangeable key ar° controlled by identifying information which is added to said digital data.".

42. Claim 69 ***additionally recites*** the limitation that; "The method according to claim 68, in which encrypting and decrypting are carried out when said identifying information is present.". The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2,lines 10-col. 8,line 51, whereas, the SVCP clearly determines identifying criteria insofar as the SVCP ' ... may be necessary to gain prior authorization before viewing of particular video... ' (i.e., col. 3,lines 13-26), as broadly interpreted by the examiner would clearly encompass ' ... identifying information is present ...'.);

Further, as per claim 80 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 69 above, and is rejected for the same reasons provided for the claim 69 rejection] according to claim 76, wherein encrypting and decrypting are carried out when said identifying information is present.".

43. Claim 70 ***additionally recites*** the limitation that; "The method according to claim 68, in which encrypting and decrypting are carried out when said identifying information is absent.".

The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2,lines 10-col. 8,line 51, whereas, the SVCP clearly determines identifying criteria insofar as the SVCP ' ... may be necessary to gain prior authorization before viewing of particular video... ' (i.e., col. 3,lines 13-26), as broadly interpreted by the examiner would clearly encompass ' ... identifying information is absent ...'.);

Further, as per claim 81 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 70 above, and is rejected for the same reasons provided for the claim 70 rejection] according to claim 76, wherein encrypting and decrypting are carried out when said identifying information is absent.".

44. Claim 71 ***additionally recites*** the limitation that; "The method according to claim 65, wherein said unchangeable key is already placed in said device.". The teachings of Davis are directed towards such limitations (i.e., col. 5,lines 60-col. 7,line 28, whereas the SVCP " ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ' ... key is already placed in said device ...' insofar as the key is used in conjunction with internal data transfer. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 82 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 71 above, and is rejected for the same reasons

provided for the claim 71 rejection] according to claim 76, wherein said unchangeable key is already placed in the device.".

45. Claim 72 ***additionally recites*** the limitation that; "The method according to claim 65, wherein said unchangeable key is generated in the device.". The teachings of Davis are directed towards such limitations (i.e., col. 5,lines 60-col. 7,line 28, whereas the SVCP " ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ' ... key is generated in said device ...' insofar as the key is used in conjunction with internal data transfer. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 83 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 72 above, and is rejected for the same reasons provided for the claim 72 rejection] according to claim 76, wherein said unchangeable key is generated in the device.".

46. Claim 73 ***additionally recites*** the limitation that; "The method according to claim 65, wherein said unchangeable key is supplied externally from the device.". The teachings of Davis are directed towards such limitations (i.e., col. 5,lines 5-col. 6,line 41, whereas the SVCP clearly re-encrypts with a user/session/ 'frame data key' prior to frame buffer storage, as broadly

interpreted by the examiner would clearly encompass ' ... key is supplied externally from said device ...' insofar as the key is a session key entered externally. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 84 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 73 above, and is rejected for the same reasons provided for the claim 73 rejection] according to claim 76, wherein said unchangeable key is supplied externally from the device.".

47. Claim 74 ***additionally recites*** the limitation that; "The method according to claim 71, 72 or 73, wherein said unchangeable key is specific to the device.". The teachings of Davis are directed towards such limitations (i.e., col. 5,lines 60-col. 7,line 28, whereas the SVCP " ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ' ... key is specific to said device ...' insofar as the key is used in conjunction with internal data transfer. Also, the SVCP is applicable to set-top box configurations which inherently have device Ids (i.e., embedded) as part of the processor PROM/ROM type memory. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise

inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 85 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 74 above, and is rejected for the same reasons provided for the claim 74 rejection] according to claim 82, 83 or 84, wherein said unchangeable key is specific to the device.".

48. Claim 75 ***additionally recites*** the limitation that; "The method according to claim 71, 72 or 73, wherein said unchangeable key is not specific to the device.". The teachings of Davis are directed towards such limitations (i.e., col. 5,lines 60-col. 7,line 28, whereas the SVCP " ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ' ... key is not specific to said device ...' insofar as the key is used in conjunction with internal data transfer. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.);

Further, as per claim 86 additionally reciting the limitation that; "] The apparatus [This claim is the apparatus claim for the method claim 75 above, and is rejected for the same reasons provided for the claim 75 rejection according to claim 82, 83 or 84, wherein said unchangeable key is not specific to the device.".

Conclusion

49. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum

Patent Examiner

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100